1. Install Java
   1. apt install default-jdk
   2. java –version [this will output: openjdk version "11.0.17" 2022-10-18….]
2. To import the Elasticsearch public GPG key into APT. Note that we are using the arguments -fsSL to silence all progress and possible errors (except for a server failure) and to allow cURL to make a request on a new location if redirected. Pipe the output of the cURL command into the apt-key program, which adds the public GPG key to APT
   1. curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –
3. Add the Elastic source list to the sources.list.d directory, where APT will search for new sources
   1. echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
4. Update your package lists so APT will read the new Elastic source
   1. apt update
5. Then install Elasticsearch
   1. apt install elasticsearch
   2. Edit /etc/elasticsearch/elasticsearch.yml and uncomment following line:
      1. network.host: localhost
   3. Start the Elasticsearch service with systemctl.
      1. systemctl start elasticsearch
   4. Run the following command to enable Elasticsearch to start up every time your server boots
      1. systemctl enable elasticsearch
   5. You can test whether your Elasticsearch service is running by sending an HTTP request
      1. curl -X GET "localhost:9200"

Output

{

"name" : "ubuntu-s-2vcpu-4gb-nyc3-01",

"cluster\_name" : "elasticsearch",

"cluster\_uuid" : "yAoTbQxXRfeUyPfGcJC2jQ",

"version" : {

"number" : "7.17.8",

"build\_flavor" : "default",

"build\_type" : "deb",

"build\_hash" : "120eabe1c8a0cb2ae87cffc109a5b65d213e9df1",

"build\_date" : "2022-12-02T17:33:09.727072865Z",

"build\_snapshot" : false,

"lucene\_version" : "8.11.1",

"minimum\_wire\_compatibility\_version" : "6.8.0",

"minimum\_index\_compatibility\_version" : "6.0.0-beta1"

},

"tagline" : "You Know, for Search"

}

1. Then install Kibana and enable and start the kibana service:
   1. apt install kibana
   2. systemctl enable kibana
   3. systemctl start kibana
2. Install nginx and allow HTTP (Optional)
   1. apt install nginx
   2. ufw allow 'Nginx HTTP'
3. Edit the following file (necessary configurations are available inside this file) to make nginx work as reverse proxy and redirect request to Kibana portal
   1. /etc/nginx/sites-available/default
   2. If it is required to change any configuration reload it after that:   
      systemctl reload nginx
4. Now Install Logstash with this command:
   1. apt install logstash
5. Create a configuration file called 02-beats-input.conf and inside it, set up your Filebeat input:
   1. touch /etc/logstash/conf.d/02-beats-input.conf

input {

beats {

port => 5044

}

}

1. Next, create a configuration file called 30-elasticsearch-output.conf
2. touch /etc/logstash/conf.d/30-elasticsearch-output.conf

output {

if [@metadata][pipeline] {

elasticsearch {

hosts => ["localhost:9200"]

manage\_template => false

index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"

pipeline => "%{[@metadata][pipeline]}"

}

} else {

elasticsearch {

hosts => ["localhost:9200"]

manage\_template => false

index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"

}

}

}

1. Start and enable Logstash
   1. systemctl start logstash
   2. systemctl enable logstash
2. Install Filebeat
   1. apt install filebeat
3. Edit filebeat configuration file: /etc/filebeat/filebeat.yml as follows:

...

#output.elasticsearch:

# Array of hosts to connect to.

#hosts: ["localhost:9200"]

...

output.logstash:

# The Logstash hosts

hosts: ["localhost:5044"]

1. Enable filebeat “nginx” module to view nginx logs from kibana
   1. filebeat modules enable nginx
2. Set up the Filebeat ingest pipelines
   1. filebeat setup --pipelines --modules nginx
3. Load the index template into Elasticsearch
   1. filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["localhost:9200"]'
4. Filebeat comes packaged with sample Kibana dashboards that allow you to visualize Filebeat data in Kibana. Before you can use the dashboards, you need to create the index pattern and load the dashboards into Kibana. As the dashboards load, Filebeat connects to Elasticsearch to check version information. To load dashboards when Logstash is enabled, you need to disable the Logstash output and enable Elasticsearch output
   1. filebeat setup -E output.logstash.enabled=false -E output.elasticsearch.hosts=['localhost:9200'] -E setup.kibana.host=localhost:5601
5. Now you can start and enable Filebeat:
   1. sudo systemctl start filebeat
   2. sudo systemctl enable filebeat
6. Verify that Elasticsearch is indeed receiving this data, query the Filebeat index with this command:
   1. curl -XGET 'http://localhost:9200/filebeat-\*/\_search?pretty'
7. To explore the Kiban, browse <http://159.203.164.255/kibana/>
8. Click the **Discover** link in the left-hand navigation bar (you may have to click the the **Expand** icon at the very bottom left to see the navigation menu items). On the **Discover** page, select the predefined **filebeat-**\* index pattern to see Filebeat data. By default, this will show you all of the log data over the last 15 minutes.
9. To view a dashboard, use the left-hand panel to navigate to the **Dashboard** page and search for the **Filebeat Nginx** dashboards. Then from the result list you can select the sample dashboards that come with Filebeat’s nginx module.